Docket No.: 33226/503001; P8951
(PATENT)

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Patent Application of:
Bhavna Bhatnagar et al.

Confirmation No.: 3673

Application No.: 10/627,019

Art Unit: 2432

Filed: July 25, 2003

Examiner: B.E. Lanier

For: METHOD AND SYSTEM FOR PROVIDING A CIRCLE OF TRUST ON A NETWORK

APPEAL BRIEF

MS Appeal Brief - Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

Dear Sir:

Pursuant to 37 CFR § 41.37, please consider the following Appellant's Brief in the referenced application currently before the Board of Patent Appeals and Interferences ("the Board").

TABLE OF CONTENTS

TABLE OF AUTHORITIES

I. REAL PARTY IN INTEREST

The real party in interest for this appeal is Sun Microsystems, Inc. An Assignment transferring all interest in the referenced application from the inventors to Sun Microsystems, Inc. was recorded by the USPTO on July 25, 2003. The Assignment is recorded at Reel 014356, Frame 0521.

II. RELATED APPEALS AND INTERFERENCES

To the best of the knowledge of the Appellants and Appellants' legal representative, there are no other appeals, interferences, or judicial proceedings which will directly affect or be directly affected by, or have a bearing on the Board's decision in this appeal.

III. STATUS OF CLAIMS

A. Total Number of Claims in Application

There are 13 claims pending in application.

B. Current Status of Claims

1. Claims canceled: 36

2. Claims pending: 13

3. Claims rejected: 13

C. Claims On Appeal

The claims on appeal are claims 37-49.

IV. STATUS OF AMENDMENTS

Appellants did not file an Amendment After Final Rejection. Thus, all of the amendments have been entered and considered by the Examiner. The pending claims of record are presented in the Claims Appendix. The claims in the Claims Appendix include the amendments filed by the Appellants on September 4, 2008.

V. SUMMARY OF CLAIMED SUBJECT MATTER

The following discussion summarizes the content of the claimed subject matter. The references to the Figures and Specification referenced below should not be construed as the only locations in the specification which support or discussion of the respective limitation.

Turning to the claims, independent claim 37 is directed to a method for granting access to a resource. *See, e.g.,* page 15 line 3 – page 16 line 3 of the originally-filed specification. The method involves sending a first authentication request to a first server. *See, e.g.,* page 15 lines 3 – 8 of the originally-filed specification. In response to the first authentication request, an authentication assertion reference is received from the first server. *See, e.g.,* page 15 lines 8-9 of the originally-filed specification. Having received the authentication assertion reference, a request to access a resource operatively connected to a second server is sent to the second server. *See, e.g.,* page 15 lines 9-11 of the originally-filed specification. Specifically, the request to access the resource includes the authentication assertion reference. *See, e.g.,* page 15 lines 9-13 of the originally-filed specification. In response to receiving the request to access the resource, the second server sends a second authentication request to the first server. *See, e.g.,* page 15 lines 14-16 of the originally-filed specification. Specifically, the second authentication request includes a certificate associated with the second server. *See, e.g.,* page 15 lines 14-16 of the originally-filed specification. Having

received the second authentication request, the first server determines whether the included certificate associated with the second server is present in a trusted partner list maintained by the first server. *See, e.g.,* page 15 lines 16-17 of the originally-filed specification. Having determined whether the certificate is present in its trusted partner list, the first server sends an authentication assertion to the second server. *See, e.g.,* page 15 line 20 – page 16 line 1 of the originally-filed specification. Once the second server has received the authentication assertion from the first server, a grant of access to the resource operatively connected to the second server is received from the second server based on the authentication assertion. *See, e.g.,* page 16 lines 1-3 of the originally-filed specification.

Independent claim 41 is directed to a method for granting access to a resource. *See, e.g.,* page 15 line 3 – page 16 line 3 of the originally-filed specification. The method involves a first server receiving a first request to access a resource operatively connected to the first server. *See, e.g.,* page 15 lines 9-11 of the originally-filed specification. Specifically, the first request includes an authentication assertion reference from a client. *See, e.g.,* page 15 lines 9-13 of the originally-filed specification. In response to receiving the first request, an authentication request is sent from the first server to the second server. *See, e.g.,* page 15 lines 14-16 of the originally-filed specification. Specifically, the authentication request includes a certificate associated with the first server. *See, e.g.,* page 15 lines 14-16 of the originally-filed specification. Upon receiving the authentication request, the second server determines whether the certificate included with the request is present in a trusted partner list maintained by the second server. *See, e.g.,* page 15 lines 16-17 of the originally-filed specification. Having determined whether the certificate is present in the trusted partner list, an authentication assertion is received at the first server from the second

server. *See, e.g.,* page 15 line 20 – page 16 line 1 of the originally-filed specification. The first server grants the client access to the resource based on the authentication assertion. *See, e.g.,* page 16 lines 1-3 of the originally-filed specification.

Independent claim 45 is directed to a system for granting access to a resource. *See, e.g.,* page 15 line 3 – page 16 line 3 of the originally-filed specification. The system includes a first server which is operatively connected to a client, a resource, and a second server. *See, e.g.,* originally-filed specification: page 14 line 17 – page 15 line 7; page 16 lines 17-21; and elements 710, 715, and 740 of Figure 7. The first server is configured to receive a request to access the resource from the client. *See, e.g.,* page 15 lines 9-11 of the originally-filed specification. Specifically, the request includes an authentication assertion reference. *See, e.g.,* page 15 lines 9-13 of the originally-filed specification. Having received the request to access the resource, the first server is further configured to send an authentication request to the second server. *See, e.g.,* page 15 lines 14-16 of the originally-filed specification. Specifically, the authentication request includes a certificate associated with the first server. *See, e.g.,* page 15 lines 14-16 of the originally-filed specification. Having received the authentication request from the first server, the second server determines whether the certificate included with the request is present in a trusted partner list maintained by the second server. *See, e.g.,* page 15 lines 16-17 of the originally-filed specification. Having determined whether the certificate is present in the second server's trusted partner list, the second server sends an authentication assertion to the first server. *See, e.g.,* page 15 line 20 – page 16 line 1 of the originally-filed specification. Having received the authentication assertion from the second server, the first server is further configured to grant the client access to the resource based on the authentication assertion. *See, e.g.,* page 16 lines 1-3 of the originally-filed specification.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The present Appeal addresses the following ground of rejection:

Whether claims 37-49 are patentable under 35 U.S.C. § 102 over U.S. Patent Publication No. 2004/0128392 ("Blakley"). For purposes of this Appeal, claims 37-49 stand or fall together. Independent claim 45 is representative of the group including claims 37-49.

VII. ARGUMENT

"A claim is anticipated only if *each and every element* as set forth in the claim is found, either expressly or inherently described, in a single prior art reference." *See* MPEP § 2131 (citing *Verdegaal Bros. v. Union Oil Co. of California*, 814 F.2d 628, 631 (Fed. Cir. 1987)) (emphasis added). Further, "[t]he identical invention must be shown in as complete detail as is contained in the claim." *See* MPEP § 2131 (citing *Richardson v. Suzuki Motor Co.*, 868 F.2d 1226, 1236 (Fed. Cir. 1989)). Accordingly, by rejecting independent claim 45 under 35 U.S.C. § 102, the Examiner contends that there are no differences between the cited prior art and the rejected claim. Appellants respectfully disagree with the Examiner's position as detailed in the forthcoming arguments. Specifically, Appellants respectfully assert that the Examiner has not properly construed the term "trusted partner list" as recited by independent claim 45. In view of these arguments presented below, Appellants respectfully assert that the Examiner's rejections should be reversed.

A. The Examiner has failed to make a proper finding that Blakley discloses every element of the rejected claim

1. The Examiner has not properly construed the term "trusted partner list"

a. Independent claim 45 recites that a trusted partner list for a first server includes a certificate associated with a second server

In re Wilson requires that all words in a claim must be considered in judging the patentability of a claim against the prior art. *See In re Wilson*, 424 F.2d 1382 (CCPA 1970). Turning to the claims, independent claim 45 explicitly recites, in part, a first server "send[ing], in response to the request, an authentication request to the second server, wherein the authentication request comprises a certificate associated with the first server." Independent claim 45 further recites, in part, a second server which "...in response to the authentication request, determines whether the certificate is present in a trusted partner list maintained by the second server." Accordingly, independent claim 45 explicitly requires that a *trusted partner list* for a first server includes a certificate associated with a second server.

b. A trusted partner list properly construed in light of the specification also discloses that a trusted partner list for a first server includes a certificate associated with a second server

Further, Appellants respectfully assert that, under *Phillips v. AWH Corp.*, the Examiner is required to read claimed limitations in light of the specification. *See Phillips v. AWH Corp.*, 415 F.3d 1303, 1313 (Fed. Cir. 2005)(en banc). Specifically, "[t]he person of ordinary skill in the art is deemed to have read the claim term not only in context of the particular claim in which the disputed term appears, but *in the context of the entire patent, including the specification.*" *See id.* Based on *Phillips* and as clearly defined by the specification, the trusted partner list for each entity includes a certificate for every other entity on the network affiliated with the particular entity. *See, e.g.,*

originally-filed specification: element 430 of Figure 4; and lines 7-18 of page 12. By way of an example, Figure 4 provides an exemplary trusted partner list for Server A, which includes certificates for Servers B and C. *See, e.g.,* originally-filed specification: element 430 of Figure 4; and line 14 page 12 – line 3 page 13. Accordingly, in agreement with a trusted partner list as defined by independent claim 45, the specification also defines that a *trusted partner list* for a first server includes a certificate associated with a second server.

2. Blakley's trust proxy is merely a registry used to maintain user credentials

Turning to the rejection, Appellants respectfully assert that, contrary to both *Wilson* and *Phillips*, the aforementioned meaning of the term "trusted partner list" was not considered by the Examiner in rejecting independent claim 45. Rather, in making the rejection, the Examiner relies upon Blakley's trust proxy to disclose the limitation of a trusted partner list. *See* page 3 line 17 – page 4 line 6 of the Final Office Action ("Final OA") dated April 13, 2009 (citing Blakley: Figure 5; and paragraphs [0070] and [0170]-[0172]). Specifically, when a user requests access to a protected resource associated with a particular domain in Blakley's federated environment (*see, e.g.*, Blakley: line 1 of paragraph [0051] – line 3 of paragraph [0052]), the trust proxy validates the user on behalf of the domain using a proof-of-possession challenge. *See* Blakley: lines 14-17 of paragraph [0170]. Further, "the content of the challenge information may require anything that *should only be possessed by the user*, such as knowledge about a username/password combination, a secret word, a hardware token such as a smartcard, a biometric identifier, etc." *See* Blakley: lines 19-24 of paragraph [0170]. Accordingly, Blakley's trust proxy, which validates a user's challenge response, is *at best* a registry which maintains user credentials. *See* Blakley: lines 1-14 of paragraph [0171].

3. Blakley's trust proxy cannot be properly construed as a trusted partner list

Independent claim 45, when read on its face and in light of the specification, requires a trusted partner list of a first server that includes a certificate associated with a second server. However, in referencing the prior art to disclose the aforementioned limitation, the Examiner relies upon Blakley's trust proxy. In view of this, Appellants respectfully assert that Blakley's trust proxy cannot be properly construed as a trusted partner list for at least the following reasons.

a. The trust proxy's user credential is not equivalent to the trusted partner list's server-associated certificate

As previously discussed, Blakley's trust proxy merely maintains user credentials to validate a user's response to a proof-of-possession challenge. Examples of user credentials include, for example, username/password combination, a secret word, a hardware token such as a smartcard, and a biometric identifier among others. *See, e.g.,* Blakley: lines 19-24 of paragraph [0170]. As such, the trust proxy *at best* maintains user-specific information pertaining to those users privileged to access protected resources through a server. In contrast, independent claim 45 requires a trusted partner list that includes a certificate associated with a server. Appellants respectfully assert that Blakley's user credentials are *merely* descriptive of a user rather than a server. Said another way, Blakley's user credentials are at best associated with a particular user who would issue a request to a server operatively connected to a protected resource. Further, Blakley is completely silent as to any association between a user credential and a server. Because a user credential cannot be said to have an association with a server, Appellants respectfully assert that a user credential cannot be properly equated with a certificate associated with a server. Accordingly, Appellants further assert that it follows that a trust proxy cannot be properly construed as a trusted partner list because of the

fundamental difference in the type of information (*i.e.*, user credentials versus server-associated certificates) maintained by each.

B. The Examiner has improperly equated a client's credentials (*i.e.*, Blakley's user) under Blakley with a server's certificate (*i.e.*, trusted partner's) even though the pending claims explicitly differentiate a client from a server as two separate entities, which perform different functions

Independent claim 45 recites, in part, that a first server is operatively connected to a client, a resource, and a second server. As such, Appellants respectfully assert that each of the aforementioned features distinctly performs a specific function[1] as recited by the claim and as described in detail by the specification. Independent claim 45 further recites, in part, that (i) a certificate is associated with the first server and that (ii) a determination is made as to whether the certificate associated with the first server is present in a trusted partner list of the second server.

Turning to the rejection, Appellants respectfully assert that the Examiner has disregarded the requirements of *In re Wilson* by equating the credentials supplied by Blakley's user (*i.e.*, a person or client) with a certificate associated with the first server. Specifically, in making the rejection, the Examiner cites to credentials provided by a user as disclosed by Blakley. *See* Final OA: page 3 lines 16-20 ("The relying domain receives credentials, that can be in certificate form, from the user and then forwards the credentials to the issuing domain (Figure 5 & [0070] & [0170]-[0171]), which meets the limitation of wherein, in response to the request, the second server sends the first server a second authentication request comprising a certificate associated with the second server" (emphasis added)). Appellants respectfully assert that, contrary to the Examiner's rejection, Blakely's

[1] Appellants invite the Board to review Appellants' Response to the Office Action dated November 18, 2008 (filed by Appellants on February 18, 2009). Appellants would like to draw the Board's attention to Annotated Figure 7 and page 3 line 6 – page 4 line 8 of the Response for further detail as to the pending claims and, more specifically, the recited client, first server, and second server features. While the aforementioned discussion is written in view of independent claim 37, Appellants respectfully submit that it is applicable to the similar limitations recited by independent claim 45.

disclosure of "credentials … in certificate form, [received] *from the user*" (*see, e.g.*, as cited in the Final OA) cannot be properly asserted to disclose the limitation of a certificate *associated with a server*. At the outset, the credential is explicitly a *user* credential according to Blakley. Further, Blakley is silent as to any association between the user credential and the relying server. Accordingly, even if the user credential were a certificate, the user credential is merely associated with the user (*i.e.*, client) and not disclosed to have an association with a *server* as required by independent claim 45. As such, the Examiner's rejection disregards independent claim 45's explicit requirement that there is a certificate which is associated with a server. Accordingly, because the Examiner is effectively reading out the limitation of the certificate's association with a server from independent claim 45, Appellants respectfully assert that the Examiner fails to consider all the words in a claim contrary to the requirements of *In re Wilson*.

C. Summary

In view of the arguments presented above, Appellants respectfully assert that Blakley does not disclose a trusted partner list as recited by independent claim 45. Because Blakley fails to disclose each and every limitation recited by independent claim 45, Appellants respectfully assert that Blakley does not anticipate independent claim 45.

VIII. Conclusion

By way of the arguments presented above, Appellants respectfully assert that the Examiner has made an improper showing that the cited prior art discloses the identical invention of independent claim 45 as required under *Richardson* and MPEP § 2131. As such, the Examiner's contentions and cited prior art do not support the rejection of the pending claims under 35 U.S.C. § 102. Accordingly, favorable consideration of the present application from the Board is respectfully requested.

Dated: October 9, 2009

Respectfully submitted,

By /Robert P. Lord/

Robert P. Lord
Registration No.: 46,479
OSHA · LIANG LLP
909 Fannin Street, Suite 3500
Houston, Texas 77010
(713) 228-8600
(713) 228-8778 (Fax)
Attorney for Appellants

601872_1

APPENDIX A

Claims Involved in the Appeal of Application Serial No. 10/627,019

1. – 36. (Canceled)

37. A method for granting access to a resource comprising:

sending a first authentication request to a first server;

receiving, in response to the first authentication request, an authentication assertion reference from the first server;

sending, to a second server, a request to access the resource operatively connected to the second server,

wherein the request comprises the authentication assertion reference,

wherein, in response to the request, the second server sends the first server a second authentication request comprising a certificate associated with the second server,

wherein the first server, in response to the second authentication request, determines whether the certificate is present in a trusted partner list maintained by the first server, and

wherein the first server, in response to determining whether the certificate is present in the trusted partner list, sends an authentication assertion to the second server; and

receiving a grant of access to the resource from the second server, wherein the second server grants access to the resource based on the authentication assertion.

38. The method of claim 37, wherein prior to sending the first server the second authentication request, the second server identifies the first server using the authentication assertion reference.

39. The method of claim 37, wherein sending a first authentication request to the first server comprises providing the first server with user login information.

40. The method of claim 39, wherein the first authentication request is a Security Assertion Markup Language request in a SOAP envelope.

41. A method for granting access to a resource comprising:

receiving, by a first server, a request to access the resource operatively connected to the first server, wherein the request comprises an authentication assertion reference from a client;

sending, in response to the request, an authentication request to a second server, wherein the authentication request comprises a certificate associated with the first server;

receiving, in response to the authentication request, an authentication assertion from the second server,

wherein the second server, in response to the authentication request, determines whether the certificate is present in a trusted partner list maintained by the second server,

wherein the second server, in response to determining whether the certificate is present in the trusted partner list, sends the authentication assertion to the first server; and

granting, by the first server, access to the resource to the client based on the authentication assertion.

42. The method of claim 41, wherein prior to sending the authentication request, the first server identifies the second server using the authentication assertion reference.

43. The method of claim 41, wherein the client is authenticated by the second server prior to obtaining the authentication assertion reference.

44. The method of claim 43, wherein the second authentication request is a Security Assertion Markup Language request in a SOAP envelope.

45. A system for granting access to a resource comprising:

a first server operatively connected to a client, the resource and a second server,

wherein the first server is configured to:

receive, from the client, a request to access the resource, wherein the request comprises an authentication assertion reference;

send, in response to the request, an authentication request to the second server, wherein the authentication request comprises a certificate associated with the first server;

receive, in response to the authentication request, an authentication assertion from the second server,

wherein the second server, in response to the authentication request, determines whether the certificate is present in a trusted partner list maintained by the second server, and

wherein the second server, in response to determining whether the certificate is present in the trusted partner list, sends the authentication assertion to the first server; and

grant access to the resource to the client based on the authentication assertion.

46. The system of claim 45, wherein the client is authenticated by the second server prior to obtaining the authentication assertion reference.

47. The system of claim 46, wherein the client provides the second server with user login information.

48. The system of claim 47, wherein the second authentication request is a Security Assertion Markup Language request in a SOAP envelope.

49. The system of claim 45, wherein prior to sending the authentication request, the first server identifies the second server using the authentication assertion reference.

APPENDIX B

No evidence pursuant to §§ 1.130, 1.131, or 1.132 or entered by or relied upon by the examiner is being submitted.

APPENDIX C

No related proceedings are referenced in II. above, hence copies of decisions in related proceedings are not provided.